What's New in Avaya Aura® Communication Manager Release 6.2, Communication Manager Messaging Release 6.2, Session Manager Release 6.3, and Branch Gateway Release 6.2

Release 6.2
03-601818
Issue 7.0
December 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's “telecommunications equipment” includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, “networked equipment”).

An “outside party” is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a “malicious party” is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company’s Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya’s customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user’s authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against

harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX

Manufacturer's Port Identifier	FIC Code	SOC/ REN/A.S. Code	Network Jacks
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242-2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive



Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 9
- Purpose 9
- Intended audience 9
- Related resources 9
  - Documentation 9
  - Training 12
  - Avaya Mentor videos 12
- Technical Assistance 13
- Support 13
- Warranty 13

Chapter 2: What's new in Communication Manager 15
- SIP to H.323 Direct Media 15
- SIP and H.323 dual registration 15
- SIP INFO out-of-band DTMF digit processing 16
- Source-based Routing 16
- International CPN Prefix 17
- Look Ahead Routing for 404 and 407 SIP Messages 17
- Signaling group usage for SIP signaling groups 17
- VDN option for DID/Tie/ISDN/SIP intercept treatment 18
- Call preservation for Communication Manager 18
- Connection Preserving Migration of SIP trunks on H.248 gateways 18
- Conference Factory URI 19
- Service Observing Next Call Listen Only Access Code 19
- Provide Agent ID 20
- Microsoft Office Communicator integration 20
- Support for Internet codec G722.2 21
- Group Paging 21
- Service Pack and Dot Release Guardian 21
- Type 3 License Allocation Algorithm 22
- Main and survivable server split registration prevention 22
- Administrable Timer for Test Type 100 23
- Patch management for Communication Manager 24
- Hardware 24
  - Supported servers 24
  - New telephones 25
- Upgrades 25
  - Upgrade paths 26
- Special applications 27

Chapter 3: What's new in Communication Manager Messaging 29
- 50-digit and variable length extensions 29
- Automatic Message Forwarding to SMTP 29
- Patch management for Communication Manager Messaging 30
- LDAP and SMTP networking 30
- SIP INFO method 31

Migration paths 31
Chapter 4: What's new in Session Manager 33
Geographic Redundancy on System Manager 33
Session Manager Role Based Access Control 33
Deny new service for entity links 34
Network parameter change 34
Terminal serviceability enhancements 34
Session identifier support 35
Chapter 5: What's new in Branch Gateway 37
Service Level Agreement Monitor 37
Appendix A: PCN and PSN notifications 39
PCN and PSN notifications 39
Viewing PCNs and PSNs 39
Signing up for PCNs and PSNs 40
Index 41

Chapter 1: Introduction

Purpose

This document provides an overview of the new and enhanced features for Avaya Aura® Communication Manager, Avaya Aura® Communication Manager Messaging, Avaya Aura® Session Manager and Avaya Branch Gateway.

Intended audience

This document is for the following audiences:

- Avaya Contractors
- Avaya Employees
- Channel Associates
- Remote Support
- Sales Representatives
- Sales Support
- On-Site Support
- Avaya Business Partners

Related resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com.

Document number	Title	Description	Audience
Implementation			
03-603558	Implementing Avaya Aura® Communication Manager	Describes the implementation instructions for Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-603560	Upgrading to Avaya Aura® Communication Manager Release 6.2	Describes procedures for upgrading Communication Manager to Release 6.2.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
18-603644	Implementing Avaya Aura® Communication Manager Messaging	Describes procedures for implementing and configuring CMM 6.2 (embedded).	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
	Operations Intelligence Suite Advanced Implementation Guide for SLA Mon	Describes Installing Service Level Agreement Monitor (SLA Mon) Server, Configuring SLA Mon Server, Uninstalling SLA Mon Server, and Backing up configuration information of SLA Mon Server.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
Administration			
555-233-504	Administering Network Connectivity on Avaya Aura® Communication Manager	Describes the network connectivity for Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-300509	Administering Avaya Aura® Communication Manager	Describes the procedures and screens used in administering	Solution Architects, Implementation Engineers, Sales

Document number	Title	Description	Audience
		Communication Manager.	Engineers, Support Personnel
Understanding			
555-245-205	Avaya Aura® Communication Manager Feature Description and Implementation	Describes the features that you can administer using Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-602878	Avaya Aura® Communication Manager Screen Reference	Describes the screen references and detailed field descriptions of Communication Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
03-603324	Administering Avaya Aura® Session Manager	Describes how to administer Session Manager using System Manager.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
555-245-207	Avaya Aura® Communication Manager Hardware Description and Reference	Describes the hardware devices that can be incorporated in a Communication Manager telephony configuration.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel
18-603645	Avaya Aura® Communication Manager Messaging Documentation CD	Describes the documentation set for Avaya Aura® Communication Manager Messaging that includes, General reference, System administration, User information, Maintenance information, and Message Manager Basics card.	Solution Architects, Implementation Engineers, Sales Engineers, Support Personnel

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Course code	Course title
AVA00383WEN	Avaya Aura® Communication Manager Overview
AVA00279WEN	Communication Manager - Configuring Basic Features
ATI01672VEN, AVA00832WEN, AVA00832VEN	Avaya Aura® Communication Manager Fundamentals
ATI02348IEN, ATI02348VEN	Avaya Aura® Communication Manager Implementation
AVA00836H00	Communication Manager Basic Administration
5U0041I	Avaya Aura® Communication Manager Administration
AVA00834WEN	Avaya Communication Manager- System Features and Administration
ATC00838VEN	Avaya Media Servers and Gateway Implementation Workshop Labs
AVA00821H00	Avaya CM Architecture and Gateways: H.248, H.323, and Proprietary
5U00104W	Session Manager 6.2 Delta Overview
5U00105W	Avaya Aura® Session Manager Overview
ATU00171OEN	Session Manager General Overview
ATC00175OEN	Session Manager Rack and Stack
ATU00170OEN	Session Manager Technical Overview
ATC01840OEN	Survivable Remote Session Manager Administration
5M00050I, 5M00050IV, 5M00050A	Avaya Aura® Communication Manager Messaging Embedded Administration, Maintenance and Troubleshooting

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Technical Assistance

Avaya provides the following resources for technical assistance.

Within the US

For help with feature administration and system applications, call the Avaya Technical Consulting and System Support (TC-SS) at 1-800-225-7585.

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to get answers to questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Warranty

Avaya provides a 90-day limited warranty on Communication Manager. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Communication Manager in the warranty period is available on the Avaya Support website at http://support.avaya.com/ under **Help & Policies** > **Policies & Legal** > **Warranty & Product Lifecycle**. See also **Help & Policies** > **Policies & Legal** > **License Terms**.

Chapter 2: What's new in Communication Manager

This chapter provides an overview of the new features and enhancements for Avaya Aura® Communication Manager 6.2, which runs on the S8300D, S8510, S8800, HP ProLiant DL360 G7, and Dell™ PowerEdge™ R610 servers.

SIP to H.323 Direct Media

Communication Manager uses the SIP to H.323 Direct Media feature to directly connect SIP stations or SIP trunks to H.323 stations, without using a media resource and shuffling the call.

When a call connects, the Direct Media feature signals a direct talk path from a SIP station or a SIP trunk to an H.323 station. The Direct Media feature can be activated on the Signaling Group screen, in the **Initial IP-IP Direct Media** field. To establish a direct path during a call setup, SIP stations and H.323 stations must use the same IP version, IPv4 or IPv6.

The benefits of using the SIP to H.323 Direct Media feature are:

- Elimination of the SIP to H.323 call shuffling after the call connects
- Elimination of clipping on the talk path
- Decrease in the number of signaling messages for each SIP to H.323 call
- Early detection of the media path in the call flow and use of fewer media processor resources to configure the system
- Reduction in the processing time of each SIP-H.323 call, and increase in the SIP Busy Hour Call Completions (BHCC) capacity

For more information on the **Initial IP-IP Direct Media** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

SIP and H.323 dual registration

With the SIP and H.323 dual registration feature, you can assign the same extension to H.323 and SIP endpoints.

When you use the same extension to register a SIP endpoint to Session Manager and an H.323 to Communication Manager, an incoming call to that extension rings at both the endpoints. The user can answer the call either at the H.323 endpoint or at the SIP endpoint.

You can create an extension of H.323 type by using System Manager. You can reassign the same extension as SIP by using the Stations with Off-PBX Telephone Integration screen in Communication Manager SAT.

For information about SIP and H.323 dual registration, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

SIP INFO out-of-band DTMF digit processing

The out-of-band option sends all outgoing DTMF messages as SIP INFO messages. When the out-of-band option is activated, Communication Manager sends SIP INFO messages over a SIP signaling group.

The out-of-band option is interoperable with H.323 networks. This option connects an Avaya non-SIP endpoint or trunk to a voicemail system on the H.323 network. The voicemail system is connected to Communication Manager and Avaya Aura® Session Manager through SIP.

For more information on the out-of-band option, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Source-based Routing

Communication Manager uses the Source-based Routing feature to send the location information of H.323, DCP, and analog stations to Session Manager.

Communication Manager includes the IP address of the caller in the bottom-most Via header of the Invite message and transmits the message to Session Manager. Session Manager uses the IP address to select the matching trunk or route pattern and then routes the call to destination stations.

To activate this feature, set the **Block sending Calling Party Location in INVITE** field to n.

Note:

This field is available only if the value of the **Group Type** field on the Trunk Group screen is sip.

For information about Source-based Routing, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878, and *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

International CPN Prefix

To convert the incoming and outgoing ISDN numbers to international format and to support international ISDN number configurations, CPN prefixes are added to the calling numbers, based on the location from where the call has originated.

The **International Access Code** field is associated with the location of the trunk on which the calling number arrives. The **International Access Code** field is administered on the Locations Parameter screen. If the **International Access Code** field is blank, Communication Manager fetches the international CPN prefix from the Feature Related System Parameter screen and adds the CPN prefix to the calling party number.

If the existing administrator option, **Passed Prefixed CPN: ASAI**, is activated, the ASAI client displays the calling party number with the CPN prefix. If deactivated, the ASAI client displays the calling party number without the CPN prefix.

For more information on the **International Access Code** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

For information on the International CPN Prefix feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Look Ahead Routing for 404 and 407 SIP Messages

When any far-end returns SIP call failure errors such as 407 (Not Found) or 404 (Proxy Authentication required), Communication Manager initiates look ahead routing (LAR), if LAR is set up correctly for the routing pattern.

Signaling group usage for SIP signaling groups

You can administer a procr near-end for SIP signaling groups the same way you administer procr near-end for H.323 signaling groups. The near-end procr set up for signaling groups works with the survivable remote, the survivable core, or the main server.

VDN option for DID/Tie/ISDN/SIP intercept treatment

The Vector Directory Number (VDN) option of the **DID/Tie/ISDN/SIP Intercept Treatment** field is now available to route incoming invalid calls to the specified VDN.

For information on the **DID/Tie/ISDN/SIP Intercept Treatment** field, see *Avaya Aura® Communication Manager Screen Reference*, 03-602878.

Call preservation for Communication Manager

A Failover Group is a group of two active Session Manager instances interconnected to ensure high availability of Session Manager services. A route pattern mechanism and a failover group domain mapping mechanism are used for call preservation during a network outage. You can administer up to nine failover domains in the Failover Group Domain Mapping (failover-grp-domain-map) table.

For preferred domain names, you can define the primary and the inverse failover groups and match them with Session Manager administration.

For more information, on call preservation administration, see *Call Preservation Administration Case Study*.

Connection Preserving Migration of SIP trunks on H.248 gateways

The Connection Preserving Migration (CPM) feature preserves existing bearer (voice) connections when a branch gateway migrates from one Communication Manager server to another because of network or server failure. However, users on connection-preserved calls cannot use features such as Hold, Conference, or Transfer. While Communication Manager and the gateways are recovering from a network or server failure, CPM extends the time period for recovery operations and functions. CPM is also supported for SIP trunks on H.248 media gateways. CPM keeps the SIP trunks on Local Survivable Processor (LSP) or Enterprise Survivability Server (ESS) in-service after the media gateway has migrated to another Communication Manager server.

Exceptions

1. Calls that do not use branch gateway resources and are shuffled to Direct-IP are not preserved.
2. SIP signaling states are not preserved for re-constructed calls. The signaling connection for the SIP call is lost as the media gateway moves over to LSP. Therefore, for re-constructed calls, the switch software does not retain signaling call states.
3. Calls that pass directly through Session Manager and not through Communication Manager are not preserved as a part of CPM call.

For more information on connection preserving migration, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Conference Factory URI

Conference Factory URI feature enables seamless integration of Session Manager with conference capabilities of conference products, such as Avaya Aura® Conferencing, Meeting Exchange, Communication Manager, and SIP endpoints, including Avaya Desktop Video Device. This feature provides enhanced experience for participants in conferences and enables richer collaboration when using voice, video, and text conference systems.

For more information, see *Administering Avaya Aura® Session Manager*, 03-603324.

Service Observing Next Call Listen Only Access Code

The Service Observing Next Call Listen Only Access Code feature is used in a call center environment where a service observer needs to monitor the observed entity. The observed entity is not notified of call monitoring, which means that there is no warning tone played and no delay when the service observer joins the call.

The service observer cannot join an active call by using this service observing feature, but can join and observe the next call. The observer can monitor calls that are routed to:

- An extension, a Vector Directory Number (VDN) on system call vectoring
- An agent who is using systems with expert agent selection

⚠ Warning:

Listening to the call of another user can be subject to federal, state, or local laws, rules, or regulations. You might need to obtain the consent of one or both of the parties on the call. Ensure that you know, and comply with, all applicable laws, rules, and regulations when you use this feature. Provision of the service observing warning tone while observing may be required in some cases. Use of the **Next Call** FAC or button will not apply warning tone even

if it is enabled for other forms of service observing and should not be used when observing calls that require the warning tone. In some cases the playing of an announcement before the call is put in queue stating that the call may be subject to monitoring will meet the legal requirements.

For more information on the Service Observing feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

For information about the maximum number of service observers on a call, see *Avaya Aura® Communication Manager System Capacities Table*.

Provide Agent ID

Using the Provide Agent ID feature, once the agent logs in to a telephone, an agent endpoint can query Communication Manager and obtain the agent ID. When the telephone receives a call center event against one of the administered lamps, the telephone initiates an agent ID inquiry message. On receiving the agent ID inquiry message, Communication Manager responds with the agent ID or, if the agent is not logged in, sends a denial event message on the extension of the agent. With accurate agent ID, the telephone can retrieve the specific agent greeting and play the greeting when a call is received. This feature is available only for Avaya 96x1 H.323 telephones.

Without accurate agent ID, the telephone cannot retrieve the Agent Greetings files. The telephone can always determine that the agent is logged in, but cannot always determine the agent ID. Without the agent ID, when a customer calls the call center to connect to a specific department, the telephone does not play the proper greeting. Due to these scenarios where the telephone might not be able to determine the agent ID, Communication Manager must send the agent ID to the telephone after the agent logs in.

Microsoft Office Communicator integration

The integration of Microsoft Office Communicator (MOC) with Communication Manager supports bridging or answering two calls simultaneously: an active call on a desk phone and an active call on an off-PBX destination, such as a mobile phone. MOC is integrated with Communication Manager by activating the **MOC Control** field on the Class of Service screen. Off-PBX Telephony Integration and Mobility (OPTIM) applications, such as CSP, EC500, PBFMC, SPFMC, and Avaya one-X® Client Enablement Services, support this feature.

With the integration of MOC, although a call to the off-PBX phone appears to be on hold to the MOC client and the desk phone, the call can be attended on both, the off-PBX phone and the desk phone. Once the off-PBX station disconnects the call, Communication Manager disconnects the call at the off-PBX phone as well as the desk phone. However, if the same call

is bridged to the off-PBX phone from the desk phone, you need to manually disconnect the call at the off-PBX phone as well as the desk phone.

For more information on administering office telephones for Extension to Cellular, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Support for Internet codec G722.2

To support high-quality audio over low-bandwidth links and also to support 96x1-series SIP Release 6.2 codec, Communication Manager provides signaling support for the G.722.2 wideband codec. The G.722.2 codec uses a 16 KHz sampling frequency and an adaptive and variable bit rate, ranging from 6.6 Kbps to 23.85 Kbps. The G.722.2 codec does not support media resources, such as Medpro and branch gateways. Communication Manager uses the G.722.2 codec to enable SIP and H.323 endpoints for direct IP calls.

For information on Administering IP Codec set, see *Administering Network Connectivity on Avaya Aura® Communication Manager*, 555-233-504.

Group Paging

SIP phones support the Group Paging feature. SIP phones not only originate a group page but also become a part of the paging group.

For information on the Group Paging feature, see *Avaya Aura® Communication Manager Feature Description and Implementation*, 555-245-205.

Service Pack and Dot Release Guardian

Avaya Service Pack and Dot Release Guardian is a patent pending technology that protects and controls the authorized use of Communication Manager service packs and dot releases by inserting the support end date (SED) in the license file and comparing it with the publication date of the service pack or dot release. The application of service packs and dot release upgrades require Avaya support entitlements. With this technology, a service pack or a dot release can be used if the publication date of the service pack or the dot release is on or before the SED in the Communication Manager license file.

For more information on Service Pack and Dot Release Guardian, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Type 3 License Allocation Algorithm

Communication Manager implements Type 3 License Allocation Algorithm during registration and unregistration. Based on the content of the license file, Type 3 License Allocation Algorithm provides multiple Type 3 feature entries for the same product ID with different releases. An available license can be used for a registered endpoint if the release number of the license is identical to the release number of the registered endpoint or a later version of the registered endpoint.

Communication Manager uses Type 3 License Allocation Algorithm to:

- Check the available capacity of the license for the same release and product ID of the registering endpoint, and uses the license based on the available capacity
- Search for available licenses of incremental releases for the product ID if adequate capacity is unavailable
- Search for any release of an available license if licenses with specific releases for the product ID are unavailable
- Release the available license at the time of unregistration

Type 3 License Allocation Algorithm is used to register licenses of multiple releases with endpoints of multiple releases. Type 3 License Allocation Algorithm provides the benefit of optimum usage of licenses and easy upgrade of the licenses for endpoints.

Type 3 License Allocation Algorithm uses the lowest-priced license for registration and releases the highest-priced license at the time of unregistration.

Main and survivable server split registration prevention

The split registration prevention feature, which ensures that gateways and telephones in a network region register to the same server, is now available for preventing split registration between the main server and the survivable core server. Earlier, this feature was only available for preventing split registration between the main server and the survivable remote servers.

The split registration prevention feature can be administered through the **Force Phones and Gateways to Active Survivable Servers** field on the IP Options System Parameters screen.

You can now administer the mg recovery rule to immediate. The functioning of immediate rule depends on the type of server the gateways are registered to. If the following conditions are met, gateways can re-register to the main server once the network stability period expires.

- The survivable server is a survivable core server.
- There are gateways registered with the main server.

The default duration of the network stability period is three minutes. You can change the duration on the mg-recovery-rule screen. If all gateways are registered with the survivable core server, the network regions assigned to the survivable server are disabled. If the survivable server is a survivable remote server, the network regions are disabled even if there are some telephones and gateways registered with the main server.

For more information on split registration, see *Administering Avaya Aura® Communication Manager*, 03-300509.

Administrable Timer for Test Type 100

The Terminating Trunk Transmission Test Type 100 timer has an administrable value. Using Test Type 100, you can test the voice quality on trunks connecting Communication Manager set up at Central Office. To test voice quality on a trunk, you can administer the time length for which the test call must be active in the **Timer** field on the Maintenance-related Systems Parameters screen.

The minimum value for the **Timer** field is 65 seconds, which is also the default value. The maximum value that you can set in this field is 999 seconds. If the trunk being tested resides on a media module board on an H.248 Gateway, the minimum value must be 300 seconds.

Test Type 100 tests far-end to near-end loss and C-message by sending a 1004 Hz tone at 0 dBm for 5.5 seconds, and then transitions to the silence mode until the call is disconnected.

For more information about the **Test Type 100** field and the **Timer** field, see *Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers*, 2403-300431.

Patch management for Communication Manager

Communication Manager supports the System Platform service pack infrastructure. You can now install the following patches and service packs, when available, by using Console Domain (cdom):

- Communication Manager dot release
- Security
- Kernel

For information on installing, downloading, and removing patches, see *Implementing Avaya Aura® Communication Manager*, 03-603558.

Hardware

Supported servers

Communication Manager runs on the following servers:

- S8300D
- S8510
- S8800
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R610

The servers mentioned in the preceding list are the ones that have the required memory and disk space to run Communication Manager on System Platform.

Only the S8300D server, HP DL360 G7, and Dell R610 are currently being sold. If you have an S8800 or S8510 server, you might need to add the necessary memory and hardware to upgrade to Communication Manager Release 6.2.

For information on the supported servers, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

New telephones

Communication Manager provides native support for the following telephones:

- 9400 series digital telephones: Avaya 9404 and Avaya 9408 digital telephones.
- 9600 series H.323 and SIP deskphones: 9608SIP, 9611SIP, 9621SIP, 9641SIP, 9608SIPCC, 9611SIPCC, 9621SIPCC, 9641SIPCC, 9608, 9611, 9621, and 9641

In addition to call processing features, Communication Manager also supports the following features for the 9400 series digital telephones:

- Fixed feature buttons, such as Hold, Conference, Transfer, Message waiting lamp, Drop and Redial
- Message button
- Customized button labels
- Forty Unicode, Eurofont, or Kanafont character display message support
- Speakerphone functionality, including Group Listen
- Support for the same set of Communication Manager call processing features that are supported by the 1416 digital deskphones

For the 9600 series H.323 and SIP deskphones, Communication Manager supports:

- Permanently labeled feature buttons, including Speaker, Mute, Volume, Headset, Contacts, Home, History, Message, and Phone.
- Languages: Arabic, Brazilian Portuguese, Simplified Chinese, Dutch, English, Canadian French, Parisian French, German, Hebrew, Italian, Japanese (Kanji, Hiragana, and Katakana), Korean, Latin American Spanish, Castilian Spanish, and Russian.

For more information on the list of telephones, see *Avaya Aura® Communication Manager Hardware Description and Reference*, 555-245-207.

Upgrades

This release of Communication Manager includes several upgrade procedures. The supported upgrade paths are listed in Upgrade paths on page 26.

For upgrade procedures, see *Upgrading Avaya Aura® Communication Manager*, 03-603560.

Upgrade paths

The following table provides the supported upgrade paths from various releases of Communication Manager to Release 6.2.

Note:

You cannot upgrade some servers to Release 4.0.5 or Release 5.2.1 directly. You must upgrade to Release 4.0.5 or Release 5.2.1 on a supported server, respectively, before you complete the upgrade to Release 6.2.

Release	Requirement
Release 1.x.x (DEFINITY R)	Restore translations to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 2.x (DEFINITY SI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.
Release 3.x.x (DEFINITY CSI)	Restore translations to an S8300D, HP DL360 G7, or Dell R610 server on Release 6.2.
Release 1.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 1.x.x (S8700)	Upgrade to Release 4.0.5 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610.
Release 2.x.x (S8300A)	Upgrade the hardware to an intermediate server (S8300B or S8300C) on Release 4.0.5 and then upgrade the hardware to S8300D Server on Release 6.2.
Release 2.x.x (S8500A, S8700, S8710 wDAL1)	Upgrade to Release 4.0.5 with memory upgrade before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610. For S8710, upgrade to Release 5.2.1 before you upgrade to Release 6.2 on HP DL360 G7 or Dell R610, You do not require to upgrade the memory.
Release 2.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 3.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.
Release 3.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 4.x.x (S8500A, S8700, S8710/S8720 wDAL1)	Upgrade to Release 4.0.5 and then upgrade to a HP DL360 G7 or Dell R610 server on Release 6.2.

Release	Requirement
Release 4.x.x (all other servers)	Upgrade to Release 4.0.5 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.0.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.1.x	Upgrade to Release 5.2.1 and then install a preupgrade service pack before you upgrade to Release 6.2.
Release 5.2.1	Install a preupgrade service pack before you upgrade to Release 6.2.
Release 6.0.x	Upgrade software-only to Release 6.2.

Special applications

Special applications, also known as green features, meet special requirements of customers. Communication Manager supports many of these special applications at no additional cost and on the same license. You can log in as a super-user and activate these applications. Although these applications are available for use, they are not extensively tested.

Some special applications require exact configuration and expert intervention. If these applications are not configured accurately, they may not operate as expected or the system may slow down or both. Avaya has identified these special applications as restricted applications. To activate these restricted applications, go to the Avaya Support website at http://support.avaya.com and open a service request.

For more information on unrestricted special applications, see *Avaya Aura® Communication Manager Special Application Features*.

Chapter 3: What's new in Communication Manager Messaging

This chapter presents an overview of the new features and enhancements for Avaya Aura® Communication Manager Messaging, which runs on the S8300D, S8510, S8800, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

Communication Manager Messaging Embedded runs on the S8300D, S8510, S8800, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

50-digit and variable length extensions

Communication Manager Messaging supports variable length mailbox extensions and extensions up to 50 digits long. The option to create the variable length extensions is available on the Switch Link screen. The variable length extension makes it easy to administer your messaging environment by allowing one-to-one mapping of real extension with mailbox numbers.

For more information, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645, and *Implementing Avaya Aura® Communication Manager Messaging*, 18-603644.

Automatic Message Forwarding to SMTP

In Communication Manager Messaging, you can have messages forwarded to:

- Microsoft Exchange
- An external SMTP account such as Yahoo! or Gmail
- Another user

By default, to prevent unwanted automatic traffic, message forwarding is disabled.

You can enable this feature by activating the **Enable automatic msg fwding** field. You must also enable it on the subscriber mailboxes.

For procedures to enable Auto Msg Fwding to SMTP, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645.

Patch management for Communication Manager Messaging

Communication Manager Messaging supports System Platform service pack infrastructure. You can now install the following patches and service packs, when available, by using cdom.

- Communication Manager Messaging dot release
- Security
- Kernel

You can download the latest patches from the Avaya Support Web site. For information on the latest patches, see *Avaya Aura®Communication Manager Release Notes*.

LDAP and SMTP networking

Communication Manager Messaging supports LDAP and SMTP networking. As a result, Communication Manager Messaging fully supports 50-digit and variable-length mailboxes.

To interact with Avaya Messaging products, such as Aura Messaging or Modular Messaging, Communication Manager Messaging does not depend on Message Networking. However, if a Communication Manager Messaging instance supporting mailboxes of more than 10 digits interacts with an earlier release of Communication Manager Messaging or Intuity Audix, it must still use Message Networking.

Both, LDAP and SMTP, are open, standard protocols. LDAP is used to transmit directory updates, whereas SMTP is used to transmit messages.

For more information on LDAP and SMTP networking, see *Avaya Aura® Communication Manager Messaging Documentation CD*, 18-603645.

SIP INFO method

Communication Manager Messaging supports DTMF transport, both inbound and outbound, by using the SIP INFO method.

The SIP INFO method transmits mid-session signaling information, such as DTMF tones along the SIP signaling path in a reliable way. The SIP INFO method uses the underlying SIP reliability. Sequenced delivery of information ensures that data packets are delivered with minimal data loss. The transmission of tones is completed during a call and is independent of the RTP.

The SIP INFO method is not used to change the state of a SIP call.

For more information on SIP INFO method, see *Implementing Avaya Aura® Communication Manager Messaging*, 18-603644.

Migration paths

Communication Manager Messaging supports the following migration paths:

- Communication Manager Messaging 4.0.5 to Communication Manager Messaging 6.2
- Communication Manager Messaging 5.2.1 to Communication Manager Messaging 6.2
- *Intuity Audix* 5.1 to Communication Manager Messaging 6.2
- *Intuity Audix* 4.4 to Communication Manager Messaging 6.2
- *Intuity Audix* LX 1.1 to Communication Manager Messaging 6.2
- *Intuity Audix* LX 2.0 to Communication Manager Messaging 6.2

For more information on migration paths, see the following documents:

- Migration from *Intuity Audix* LX R2.0 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603650
- Migration from *Intuity Audix* LX R1.1 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603649
- Migration from *Intuity Audix* R5.1 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603648
- Migration from *Intuity Audix* R4.4 to *Avaya Aura®Communication Manager Messaging* R6.2, 18-603646

Communication Manager Messaging 6.0 and 6.0.1 support upgrades to Communication Manager Messaging release 6.2. For upgrading procedures, see *Upgrading Avaya Aura® Communication Manager*, 03-603560.

Chapter 4: What's new in Session Manager

This chapter presents an overview of the new features and enhancements for Avaya Aura® Session Manager, which runs on the S8300D, S8510, S8800, Dell™ PowerEdge™ R610, and HP ProLiant DL360 G7 servers.

Geographic Redundancy on System Manager

Session Manager supports the System Manager Geographic Redundancy feature, which provides increased system reliability and robustness by ensuring that enterprise communications and management capability are not impacted by the failure of a single System Manager instance or the failure of the network.

The System Manager Geographic Redundancy feature consists of two System Manager instances, running in locations that are geographically remote from each other, working to control System Manager and other network elements. The two instances of System Manager are referred to as the primary System Manager instance and the secondary System Manager instance. In normal operations, the primary System Manager instance controls the system and synchronizes the database of the primary System Manager instance with the database of the secondary System Manager instance.

If the primary System Manager server fails or loses network connectivity, then the primary System Manager cannot administer System Manager, so the secondary System Manager instance administers all the associated network elements. Once the primary System Manager instance is available again, it takes control of the network elements.

For information about System Manager Geographic Redundancy, see *Administering Avaya Aura® Session Manager Release 6.3*.

Session Manager Role Based Access Control

With Role Based Access Control (RBAC), you can have role-based capabilities for administrators of Session Manager. You can assign the following roles: Network Administrator, System Administrator, and Avaya Services Administrator. You can also create custom roles for Routing and Session Manager Administration modules.

For information about roles, see *Administering Avaya Aura® Session Manager Release 6.3*.

Deny new service for entity links

With the Deny new service for entity links feature, entity links do not accept new incoming calls and Session Manager does not route outgoing calls over them. Link monitoring continues over these links but no alarms are generated for the denied links.

This feature is useful when you:

- Take selected SIP entities out of service for upgrades and repair and do not want SIP monitoring alarms to be raised.
- Isolate a branch to its survivable server during WAN fluctuations or data center maintenance.
- Test alternate routing paths by denying the primary link used on a given route.
- Plan a WAN outage.

For information about Deny new service for entity links, see *Administering Avaya Aura® Session Manager Release 6.3*.

Network parameter change

When a user changes the IP address of System Manager, Session Manager receives a notification. Session Manager replaces the new address throughout the database for all instances. Similarly, when a user changes the IP address of Session Manager, System Manager receives a notification of the change in the IP address and updates the database with the new IP address.

Terminal serviceability enhancements

You can use System Manager to log in to a single SIP terminal or a group of SIP terminals. Using System Manager, you can enter and manage the SSH passwords and parameters on all SIP telephones. System Manager provides the functionality to store labels for buttons for different set types.

The enhancements to the SIP terminal are:

- **Display of last reboot or reset**: SIP registration page displays the downtime after you reset or restart a SIP telephone.
- **Display name download for contact list**: Session Manager sends the administered Endpoint Display Name of the contacts in the contact list to the SIP endpoints.
- **Auto abbreviated or delayed transition interval**: Session Manager sends the Auto Abbreviated or the Delayed Transition Interval (rings) message to SIP endpoints. Endpoints that are administered with abbreviated ringing or delayed ringing receive the number of ring cycles before automatic transition to silence. For abbreviated ringing, the station is in the audible ringing mode for the administered number of ring cycles and then changes over to the silent mode until the call is covered. For delayed ringing, the station rings in the silent mode for the administered number of ring cycles and then changes over to the audible ringing mode.

Session identifier support

With this feature, Session Manager labels each point-to-point session with a globally unique identifier. After receiving an initial request, Session Manager generates a 128-bit identifier and inserts the identifier in the Global-Session-ID header of the request.

Session Manager labels and logs the association between point-to-point sessions, stores the header of the request message, and then updates the Global-Session-ID header. Using a tracing tool, you can filter out the relevant logged messages for troubleshooting call flows.

Chapter 5: What’s new in Branch Gateway

This chapter provides an overview of new features for Avaya Branch Gateway.

Service Level Agreement Monitor

Service Level Agreement (SLA) Monitor is an integrated set of tools designed to help obtain the highest end-to-end audio and video performance on a converged network. SLA Monitor communicates with agents embedded in the components of IP telephony and other sources through a web-based server application. With the data gathered by SLA Monitor through this communication, you can check the networks contribution to the performance of audio and video applications.

SLA Monitor helps:

- Correct Differentiated Services (DiffServ) issues.
- Handle rogue applications.
- Provide real-time visibility to live sessions.

The SLA Monitor agent is a component of SLA Monitor. The agent participates in the enterprise end-to-end monitoring and troubleshooting of various types of network problems that affect IP telephony. The SLA Monitor agent traces packets from source to destination and monitors the DiffServ markings at each hop as the packets travel through the network.

The SLA Monitor server, which is also part of SLA Monitor, collects router flow data as well as data from the SLA Monitor agents to help produce a clear picture of how the network and the media elements contribute to end-to-end quality.

Branch Gateway G430 and Branch Gateway G450 act as the SLA Monitor agents.

For more information on the SLA Monitor server and agent, see *Operations Intelligence Suite Advanced Implementation Guide for SLA Mon*.

Appendix A: PCN and PSN notifications

PCN and PSN notifications

Avaya issues a product-change notice (PCN) in case of any software update. For example, a PCN must accompany a service pack or a patch that needs to be applied universally. Avaya issues product-support notice (PSN) when there is no patch, service pack, or release fix, but the business unit or services need to alert Avaya Direct, Business Partners, and customers of a problem or a change in a product. A PSN can also be used to provide a workaround for a known problem, steps to recover logs, or steps to recover software. Both these notices alert you to important issues that directly impact Avaya products.

Viewing PCNs and PSNs

About this task

To view PCNs and PSNs, perform the following steps:

Procedure

1. Go to the Avaya Support website at http://support.avaya.com.

   Note:

   If the Avaya Support website displays the login page, enter your SSO login credentials.

2. On the top of the page, click **DOWNLOADS & DOCUMENTS**.
3. On the Downloads & Documents page, in the **Enter Your Product Here** field, enter the name of the product.
4. In the **Choose Release** field, select the specific release from the drop-down list.
5. Select **Documents** as the content type.
6. Select the appropriate filters as per your search requirement. For example, if you select Product Support Notices , the system displays only PSNs in the documents list.

Note:

You can apply multiple filters to search for the required documents.

Signing up for PCNs and PSNs

About this task

Manually viewing PCNs and PSNs is helpful, but you can also sign up for receiving notifications of new PCNs and PSNs. Signing up for notifications alerts you to specific issues you must be aware of. These notifications also alert you when new product documentation, new product patches, or new services packs are available. The Avaya E-Notifications process manages this proactive notification system .

To sign up for notifications:

Procedure

1. Go to the Avaya Support Web Tips and Troubleshooting: eNotifications Management page at https://support.avaya.com/ext/index?page=content&id=PRCS100274#.
2. Set up e-notifications. For detailed information, see the **How to set up your E-Notifications** procedure.

Index

Numerics

404 SIP messages 17
407 SIP messages 17
50-Digit extensions 29
96x1 H.323 telephones 20

A

Administrable Timer Test Type 100 23
agent ID 20
Allocating Type 3 licenses 22
audience 9
Automatic Message Forwarding to SMTP 29
Avaya Desktop Video Device 19
Avaya Mentor videos 13

C

Call preservation 18
Communication Manager 15
Communication Manager Messaging 29
Conference Factory URI 19
Conferencing 19
connection preserving migration 18

D

Deny new service for entity links 34
description 21
dual registration 15

F

Feature Access Code (FAC) 19

G

Geographic redundancy 33
Group Paging 21

I

International CPN Prefix 17

L

LDAP and SMTP networking 30
legal 2

M

Main and survivable server split registration prevention 22
Meeting Exchange 19
Microsoft Office Communicator integration 20
Migration paths 31

N

Network parameter change 34
New telephones 25

P

Patch management for Communication Manager 24
Patch management for Communication Manager Messaging 30
PCN 39
PCN notification 39
PCNs 39
PSN 39
PSN notification 39
PSNs 39

R

related documentation 10
related resources 13
    Avaya Mentor videos 13

S

Service Observing Next Call Listen Only Access Code 19
Service Pack and Dot Release Guardian 21
Session identifier support 35
Session Manager 33
Session Manager Role Based Access Control 33
signing up for PCNs and PSNs 40
SIP and H.323 dual registration 15

SIP INFO method 31
SIP INFO out-of-band DTMF digit processing 16
SIP signaling group 17
SIP to H.323 Direct Media 15
SIP trunks 18
SMTP networking 30
Source-based Routing 16
Special applications 27
support 13
contact 13
Support for Internet codec G722.2 21
Supported servers 24

T

technical assistance 13
Terminal serviceability enhancements 34
training 12

U

upgrade paths 26
Upgrade paths 31
Upgrades 25

V

Variable-length Extensions 29
VDN option for DID/Tie/ISDN/SIP Intercept Treatment 18
videos 13
Avaya Mentor 13

W

Warranty 13
What's new audience 9
What's new in Communication Manager 15
What's new in Communication Manager Messaging ..29
What's new in Session Manager 33
What's New overview 9